BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) Japanese Patent Office (JP)
(12) Publication of Patent Applications (A)
(11) Patent application publication number
Kokai (unexamined patent publication) NO. 9-6681
(43) Publication date: January 10, 1997
Domestic classification symbol
Reference No.
Technology indication area
Request for examination
Not requested
Number of claims
(Seven pages in total)
(21) Application No.: Patent application No.7-174510
(22) Filing date: June 15, 1995
(71) Applicant: 000000952
Kanebo, LTD.
5-17-4, Sumida, Sumida-ku, Tokyo
(72) Inventor: Yoichi Nakamura
1-6-9-502, Tomobuchi-cho, Toshima-ku, Osaka
(54) Title of the Invention
Apparatus and method for checking top secrecy in a data management system

(57) [Abstract]
[Purpose] To provide an apparatus and method for checking the protection of top secrecy that one operator can operate easily and promptly with a plurality of authority when performing data operation

[Constitution] An apparatus that checks the protection of top secrecy with regard to an operator when he retrieves the data that he desires from a plurality of groups of data stored as a group of data concerning a plurality of relevant items comprises an authority setting unit (2 and 7) setting a plurality of kinds of authority that establishes an operable range concerning items and/or operation contents and assigning the kind of authority

for each operator to each data group; and a judgement unit (3) retrieving the operator's authority from the authority setting unit (2 and 7) after receiving the identification information of the operator and operation contents that are inputted by an input unit, and judging that if the operator has the authority to operate the data that he desires, it is possible to retrieve the data and that if he does not have said authority, it is not possible to retrieve the data.

[Scope of claim for patent]

[Claim 1] A method for checking the protection of top secrecy with regard to an operator in a data management system when he retrieves the data that he desires from a plurality of groups of data stored as a group of data concerning a plurality of relevant items, comprising the steps of:

setting a plurality of kinds of authority that establishes an operable range concerning items and/or operation contents and assigning the kind of authority for each operator to each data group; and

checking the operator's authority for the data that he desires and judging that if the operator has the authority to operate the data that he desires, it is possible to retrieve the data and that if he does not have said authority, it is not possible to retrieve the data.

[Claim 2] An apparatus that checks the protection of top secrecy with regard to an operator in a data management system when he retrieves the data that he desires from a plurality of groups of data stored as a group of data concerning a plurality of relevant items, comprising:

an authority setting unit (2 and 7) setting a plurality of kinds of authority that establishes an operable range concerning items and/or operation contents and assigning the kind of authority for each operator to each data group; and

a judgement unit (3) retrieving the operator's authority from the authority setting unit (2 and 7) after receiving the

identification information of the operator and operation contents that are inputted by an input unit, and judging that if the operator has the authority to operate the data that he desires, it is possible to retrieve the data and that if he does not have said authority, it is not possible to retrieve the data.

[Detailed description of the invention]

[0001]

[Field of Industrial application] The present invention relates to an apparatus and method for checking the protection of top secrecy with regard to an operator when he retrieves the data that he desires from a plurality of groups of data that are stored as a group of data concerning a plurality of relevant items.

[0002]

[Prior art] In general, a computer-aided system deals with a wide range of information and a large amount of information, and a lot of operators are involved in the operation of the system. It is necessary, therefore, to limit a free use of the system for important information. In order to prevent each operator from using the important information illegally or updating the important information illegally, a mechanism for protecting top secrecy that limits the operable range of the system for each operator is provided. In the past, however, this check of the protection of top secrecy was conducted using an operator's "user name and password," etc.

[0003]

Described below are the details of an example of this prior art with reference to Fig. 7 and Fig. 9. First, ID code and password for each operator as well as authority for each password are determined as shown in Fig. 7. Also, the operable range for each authority is determined as shown in Fig. 8. Then, the process of checking the protection of top secrecy is performed when the operator conducts data operation, as shown in Fig. 9. That is, the operator inputs his ID code and password (Step S201). The system checks whether the inputted ID code and password are correct (Step S202). If the inputted ID and password are correct,

the system obtains the operator's authority from the determined authority (Step S203). When an operation target document and operation contents are inputted by the operator (Step S204), the system judges whether the operator can perform the inputted operation from the contents of the authority shown in Fig. 8 (Step S205), and if the judgement is YES, the system enables the operator to perform the inputted operation (Steps S206, S207, S209). In the past, therefore, when operation was performed with any different authority, it was not until the operator inputted the ID code and password corresponding to said authority again and obtained necessary authority that he could carry out the operation (Step S209).

[0004]

[Problems to be solved by the invention] In the check of the protection of top secrecy by means of prior art, an operator was identified by "user name and password" and then the check was implemented, so the operable authority of the system was subordinate to the operator, and one operator was unable to perform a simultaneous operation with a plurality of authorities. Thus, the operator had to log in the "user name and password" responding to another authority again, so such a method is employed that after the process of checking the protection of top secrecy is passed again, the process proceeds to another authority. Consequently, the operation was complicated and it was difficult to conduct rapid processing.

[0005]

The present invention was realized in the light of said circumstances with the aim of providing an apparatus and method for checking the protection of top secrecy that one operator can operate easily and promptly with a plurality of authorities when performing data operation.

[0006]

[Means for solving the problem] The invention according to claim 1 is the method for checking the protection of top secrecy with regard to an operator in a data management system when he retrieves the data that he desires from a plurality of groups of data stored

as a group of data concerning a plurality of relevant items, comprising the steps of:

setting a plurality of kinds of authority that establishes an operable range concerning items and/or operation contents and assigning the kind of authority for each operator to each data group; and

checking the operator's authority for the data that he desires and judging that if the operator has the authority to operate the data he desires, it is possible to retrieve the data and that if he does not have said authority, it is not possible to retrieve the data.

[0007]

Also, the invention according to claim 2 is the apparatus that checks the protection of top secrecy with regard to an operator in a data management system when he retrieves the data that he desires from a plurality of groups of data stored as a group of data concerning a plurality of relevant items, comprising:

an authority setting unit setting a plurality of kinds of authority that establishes an operable range concerning items and/or operation contents and assigning the kind of authority for each operator to each data group; and

a judgement unit retrieving the operator's authority from the authority setting unit after receiving the identification information of the operator and operation contents that are inputted by an input unit, and judging that if the operator has the authority to operate the data he desires, it is possible to retrieve the data and that if he does not have said authority, it is not possible to retrieve the data.

[0008]

[Operation] According to the invention according to claims 1 and 2, the authority setting unit sets a plurality of kinds of authority that establishes an operable range concerning items and/or operation contents and assigns the kind of authority for each operator to each data group. Then, the operator inputs his identification information and operation contents into the

judgement unit. Receiving the identification information and operation contents, the judgement unit retrieves the authority of the operator. If the operator has the authority to operate the data that he desires, the judgement unit judges that it is possible to retrieve the data, and if he does not have said authority, the judgement unit judges that it is not possible to retrieve the data.

[0009]

Thus, according to the present invention, different kinds of authority for each data group can be set for one operator. As a result, the protection of top secrecy can be checked for each data group, and the protection of top secrecy does not need to be checked for all data, so that it is possible to check the protection of top secrecy easily and promptly.

[0010]

[Embodiment] Described below are the details of an embodiment of the present invention with reference to the accompanying drawings. Fig. 1 shows the schematic diagram of an apparatus embodying the present invention. This apparatus is a filing apparatus that files document data, etc. and has a mechanism for checking the protection of top secrecy with regard to an operator of the apparatus (hereinafter referred to as "user"). This apparatus comprises a CPU (1), a storage device (5), an input device (9) and a display device (10). The CPU (1) comprises an authority registration unit (2), an authority retrieval/judgement unit (3) and a process execution unit (4). The storage device comprises a data storage unit (6), an authority information storage unite (7) and a processing program unit (8). Described below are the details of each device and unit. The input device (9) comprises a keyboard, a mouse, etc., and the display device (10) comprises a display, etc., all of which are so well known that the details of theses devices are omitted. Also, in this embodiment, document data are used as the data to be filed, but the things that are filed are not limited to document data, but can be numerical data.

[0011]

The processing program unit (8) stores a program for executing a designated process, and the process execution unit (4) reads a program corresponding to a designated process from the processing program unit (8) and executes the program.

[0012]

The authority registration unit (2) receives inputted information from the input device (9) and sets a plurality of authority that prescribes the operable range that a user can operate and assigns the kinds of said authority to each user. Described below are further details of the function of the authority registration unit (2) with reference to Fig. 2 and Fig. 3. Fig. 2 is a table showing the setting of the kind of authority. Fig. 3 is a table showing the assignment of authority. Concerning the document data in this embodiment, a plurality of kinds of document (quotation and contract) data are presumed to exist for each theme (e.g. for each customer). This "each document data" corresponds to "items" specified in Claims 1 and 2, and "a plurality of document data for each theme" corresponds to "data group" specified therein.

[0013]

First, described below is the setting of authority. In this embodiment, the authority is divided into "manager authority" and "person-in-charge authority," as shown in Fig. 2, and respective contents are set for both of the authority. That is, "manager authority " can conduct operation for approval of quotation documents and approval of contract documents, but cannot conduct operation for making or change of quotation documents and making or change of contract documents, while "person-in-charge authority" can conduct operation for making or change of quotation documents and making or change of contract documents, but cannot conduct operation for approval of quotation documents and approval of contract documents. "Making," "change" and "approval" referred hereto correspond to "operation contents" specified in claims 1 and 2. Thus, the setting of authority is implemented by setting whether "operation contents" related to "documents data" can be operated or not.

[0014]

Fig. 3 shows which authority each user has for each theme, "manager authority" or "person-in-charge authority." For example, "staff A" who is one of the users has "person-in-charge authority" for theme 1, has "manager authority" for theme 2, and has "manager authority" and "person-in-charge authority" for theme 3. Thus, the assignment of authority is implemented by assigning authority to each user for each theme.

[0015]

The data storage unit (6) stores the document data, and the authority information storage unit (7) stores the authority information set by the authority registration unit.

[0016]

The authority retrieval/judgement unit (3) obtains a user's identification information and information concerning a theme and retrieves the authority information storage unit (7) based on said information to obtain the user's authority information, and then judges whether the user can retrieve the document data that he designates based on said authority information.

[0017]

Described below are further details of this judgement processing with reference to Fig. 4. "Staff A" who is one of the users inputs his user name and password from the input unit (9) to log in (Step S1), as shown in Fig. 4. Then, the authority retrieval/judgement unit (3) judges that the user is "staff A" from the user name and password. At that time, if the password for the user is not correct, an error occurs, thereby making it impossible for the user to log in. In succession, "staff A" selects the theme that he operates ("theme 1" in this example) from among the themes that he is in charge of, and inputs the selected theme (Step S2). The authority retrieval/judgement unit (3) retrieves the authority information storage unit (7) and obtains the kind of authority of "staff A" and the contents of the authority (Step 3). In this case, however, it is presumed that "staff A" can select only the theme for which he has the authority, and cannot select any theme for which he does not

have the authority. "Staff A" has the authority for "theme 1," "theme 2" and "theme 3," but does not have any authority for "theme 4," as shown in Fig. 3. So, "staff A" can select "theme 1," "theme 2" and "theme 3," but cannot select "theme 4." In the example shown in Fig. 4, "theme 1" is selected, and the authority retrieval/judgement unit (3) obtains the information to the effect that the authority of "staff A" is "person-in-charge authority" from the authority information storage unit (7).
[0018]

"Staff A" successively selects and inputs the contents of operation that he desires. Receiving the inputted contents of operation, the authority retrieval/judgement unit (3) compares the contents of authority obtained from the authority information storage unit (7) and the inputted contents of operation. If "staff A" can operate said processing, the authority retrieval/judgement unit (3) outputs a signal of "operable" to the process execution unit (4), and if "staff A" cannot operate said processing, the authority retrieval/judgement unit (3) displays "inoperable" on the display device (10). The process execution unit (4) reads the processing program fitting the selected process from the processing program unit (8) of the storage device (5), and executes said program (Step S4). In the example shown in Fig. 4, "staff A" can conduct operation for the making or change of the quotation or the making or change of the contract, but cannot conduct operation for the approval of the quotation or the approval of the contract.
[0019]

Fig. 5 shows an example in which the user changes his theme after logging in. In this example, after logging in, the user can change his theme at any time. However, when he tries to change his theme after logging in, he cannot conduct operation for any other theme with which he has nothing to do. Since the theme that "staff A" can select is "theme 1," "theme 2" and "theme 3," as described above, the user cannot conduct operation for any theme other than these themes. When he changes his theme, the authority retrieval/judgement unit (3) automatically

obtains the authority in which the user is assigned to said theme according to the theme that the user selects and changes the authority. In the example shown in Fig. 5, when the user's theme is changed to "theme 2," the authority is automatically changed to "manager authority," and when it is changed to "theme 3," the authority is automatically changed to "manager authority + person-in-charge authority." Then, the user can conduct operation in accordance with this authority.

[0020]

Fig. 6 shows a series of these processes.

[0021]

[Effect of the invention] According to the present invention, different kinds of authority for each data group can be set for one operator. As a result, the protection of top secrecy can be checked for each data group, and the protection of top secrecy does not need to be checked for all data, so that it is possible to check the protection of top secrecy easily and promptly. Also, a plurality of authority can be set for one operator, so a further detailed check of the protection of top-secret can be implemented and a prompt transfer to a different kind of authority can be also implemented, thus allowing prompt operation of the system.

[Brief description of the drawings]

Fig. 1 is a block diagram showing the rough configuration of an apparatus embodying the present invention.

Fig. 2. is a table showing the kind of authority.

Fig. 3 is a table showing the assignment of authority.

Fig. 4 is a flowchart showing the contents of the process of performing judgement.

Fig. 5 is a flowchart showing the contents of the process of changing a theme after a user logs in.

Fig. 6 is a flowchart showing the contents of the process of performing judgement and changing a theme.

Fig. 7 is a table showing the relationship between ID codes, etc. and authority.

Fig. 8 is a table showing the kind of authority.

Fig. 9 is a flowchart showing the process of checking the protection of top secrecy with an apparatus involving prior art.

[Explanations of numerals]

1 CPU
2 Authority registration unit
3 Authority retrieval/judgement unit
4 Process execution unit
5 Storage device
6 Data storage unit
7 Authority information storage unit
8 Processing program unit
9 Input device
10 Display device

Fig. 1

10 Display

1 CPU

2 Authority registration unit

3 Authority retrieval/judgement unit

4 Processing execution unit

9 Input device

5 Storage device

6 Data storage unit

7 Authority information storage unit

8 Processing program unit

Fig. 2

Operable range for each kind of authority

	Manager authority	Person-in-charge authority
Making and change of quotation document	Not possible	Possible
Approval of quotation document	Possible	Not possible
Making and change of contract document	Not possible	Possible
Approval of contract document	Possible	Not possible

Fig. 3

Authority for each theme of an operator

	Theme 1	Theme 2	Theme 3	Theme 4
Staff A	Person in charge	Manager	Manager and Person in charge	
Staff B	Manager	Person in charge	Person in charge	
Staff C	Person in charge	Person in charge	Person in charge	

Fig. 4

S1 Staff A logs in.

S2 Staff A selects his target theme.

S3 The authority retrieval/judgement unit obtains the authority of the theme that he selects.

S4 The processing execution unit checks the protection of top secrecy.

① Operator Staff A

② Operator Staff A Theme Theme 1

③ Operator Staff A Theme Theme 1 Authority Person in charge

④

	Operation by person-in-charge authority
Making and change of quotation document	Possible
Approval of quotation document	Not possible
Making and change of contract document	Possible
Approval of contract document	Not possible

Fig. 5

① Operator Staff A

② Change of theme

Operator Staff A Operator Staff A Operator Staff A

Theme Theme 1 Theme Theme 2 Theme Theme 3

③ Authority = Person in charge

Authority = Manager

Authority = Person in charge and manager

④

Making and change of quotation document

Approval of quotation document

Making and change of contract document

Approval of contract document

Operation by person-in-charge authority

Possible

Not possible

Possible

Not possible

Operation by manager authority

Not possible

Possible

Not possible

Possible

Operation by person-in-charge and manager authority

Possible

Possible

Possible

Possible

Fig. 6

① Staff A logs in.

② Staff A selects his target theme.

③ The authority retrieval/judgement unit obtains the authority of the theme that he selects.

④ The processing execution unit checks the protection of top secrecy.

Start

S101 Staff A inputs his ID code and password.

S102 The authority retrieval/judgement unit judges whether the ID code and password are correct.

S103 Staff A selects the theme that he operates.

S104 Is operation possible?

S105 The authority retrieval/judgement unit obtains the authority in which staff A is assigned to the theme.

S106 The authority retrieval/judgement unit selects the document and contents of operation.

S107 Is operation allowable?

S108 Can staff A conduct operation for the making of document?

S109 Does the operation terminate?

S110 Does staff A change his theme?

S111 End

Fig. 7

Authority for each password of an operator

Operator ID	Password	Operator authority
Staff A	123	Person-in-charge
Staff B	124	Manager
Staff C	456	Manager
Staff D	789	Person-in-charge

Fig. 8

Operable range for each kind of authority

	Manager authority	Person-in-charge authority
Making and change of quotation document	Not possible	Possible
Approval of quotation document	Possible	Not possible
Making and change of contract document	Not possible	Possible
Approval of contract document	Possible	Not possible

Fig. 9

Start

S201 Operator inputs his ID code and password.

S202 The system checks whether the ID code and password are correct.

S203 The system obtains the operator's authority.

S204 The system receives the input of document and operation contents.

S205 The system judges whether the operator can perform the input operation.

S206 The system operates the document.

S207 Does the operation terminate?

S208 End

S209 Is operation conducted with a different kind of authority?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－6681

(43)公開日　平成９年(1997)１月10日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３１０		Ｇ０６Ｆ	12/14	３１０Ｋ
	12/00	５３７	7623－5B		12/00	５３７Ａ

審査請求　未請求　請求項の数２　ＦＤ　（全　７　頁）

(21)出願番号　特願平7－174510

(22)出願日　平成７年(1995)６月15日

(71)出願人　000000952
鐘紡株式会社
東京都墨田区墨田五丁目17番４号

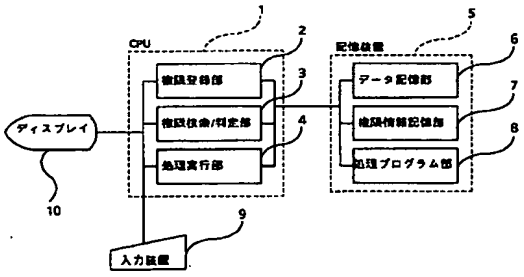
(72)発明者　中村　洋一
大阪市都島区友渕町１丁目６番９－502号

(54)【発明の名称】　データ管理装置における機密チェック方法および装置

(57)【要約】

【目的】データ操作を行う際に、一人の操作員が簡易かつ迅速に複数の権限で操作を行うことのできる機密保護のチェック方法及び装置を提供する。

【構成】関連ある複数の項目についての１群のデータとして記憶した複数群のデータから操作員が所望のデータを検索する際に、該操作員について機密保護のチェックを行う装置であって、項目及び／又は操作内容について、操作可能な範囲を定めた複数種類の権限を設定するとともに、各操作員について、各データ群毎に権限の種類を割り付ける権限設定手段（２，７）と、入力手段（９）より入力された操作員の識別情報及び操作内容を受けて、権限設定手段（２，７）から該操作員の権限を検索し、所望したデータの操作について該操作員が権限を有するならば該データの検索を可能と判定し、権限を有しないならば検索を不可能と判定する判定手段（３）とから構成する。



1

【特許請求の範囲】

【請求項１】　関連ある複数の項目について１群のデータとして記憶した複数群のデータから操作員が所望のデータを検索する際に、該操作員について機密保護のチェックを行う方法であって、

前記項目及び／又は操作内容について、操作可能な範囲を定めた複数種類の権限を設定するとともに、

各操作員について、前記各データ群毎に前記権限の種類を割り付け、

データ検索時に、該操作員が所望した該データについての該操作員の権限をチェックし、該操作員が該データについて権限を有するならば該データの検索を可能とし、権限を有しないならば検索を不可能とすることを特徴とするデータ管理装置における機密チェック方法。

【請求項２】　関連ある複数の項目についての１群のデータとして記憶した複数群のデータから操作員が所望のデータを検索する際に、該操作員について機密保護のチェックを行う装置であって、

前記項目及び／又は操作内容について、操作可能な範囲を定めた複数種類の権限を設定するとともに、各操作員について、前記各データ群毎に前記権限の種類を割り付ける権限設定手段と、

入力手段より入力された操作員の識別情報及び操作内容を受けて、前記権限設定手段から該操作員の権限を検索し、所望したデータの操作について該操作員が権限を有するならば該データの検索を可能と判定し、権限を有しないならば検索を不可能と判定する判定手段とから構成したことを特徴とするデータ管理装置における機密チェック装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、関連ある複数の項目について１群のデータとして記憶した複数群のデータから操作員が所望のデータを検索する際に、該操作員について機密保護のチェックを行う方法及び装置に関する。

【０００２】

【従来の技術】一般にコンピュータシステム装置においては多種，多様且つ大量の情報を扱っており、またその操作においても多くの操作員が関与しているので、重要な情報に対しては自由な利用を制限する必要がある。そのため、かかる重要な情報に対しては、不正使用・不正更新を防止すべく各操作員に対して利用できる操作範囲を制限する機密保護の仕組を講じている。従来、この機密保護のチェックは操作員の「ユーザ名及びパスワード」等を用いて行われていた。

【０００３】この例を図７乃至９を用いて詳細に説明する。まず、図７に示すように、各操作員についてＩＤコード及びパスワードとその権限を取り決める。また、図８に示すように各権限についてその操作可能な範囲を取り決める。そして、図９に示すように、データ操作に際して機密保護チェックの処理を行う。即ち、まず、操作員が自らのＩＤコード及びパスワードを入力する（ステップＳ２０１）。これを受けて入力されたＩＤコード及びパスワードが正しいか否かをチェックし（ステップＳ２０２）、正しければ前記権限の取り決めから当該操作員の権限を獲得する（ステップＳ２０３）。操作員からの操作対象書類及び操作内容の入力を待って（ステップＳ２０４）、図８に示した権限内容から、入力された操作を当該操作員が実行可能かどうかを判断し（ステップＳ２０５）、実行可能であれば当該操作を可能ならしめる（ステップＳ２０６，Ｓ２０７，Ｓ２０９）。そして、従来、異なる権限で操作を行う際には、操作員は再び当該権限に対応したＩＤコード及びパスワードを入力し、必要な権限を獲得した後でなければこれを実行することができなかった（ステップＳ２０９）。

2

【０００４】

【発明が解決しようとする課題】このように、従来の機密保護チェックにおいては、「ユーザー名及びパスワード」により操作員を特定しチェックするといったように、その操作可能権限は操作員に従属しており、１人の操作員が複数の権限で同時に操作を行うことが不可能であった。かかる場合に、叙上のように当該操作員は別の権限に対応した「ユーザー名及びパスワード」で再びログインするといったように、機密保護チェックの処理を再度通過して別の権限に移行する方法を採っていたため、その操作が煩雑であり、迅速な処理が困難であった。

【０００５】本発明は以上の実情に鑑みなされたものであって、データ操作を行う際に、一人の操作員が簡易かつ迅速に複数の権限で操作を行うことのできる機密保護のチェック方法及び装置の提供を目的とする。

【０００６】

【課題を解決するための手段】上記目的を達成するための本発明の請求項１にかかる発明は、関連ある複数の項目について１群のデータとして記憶した複数群のデータから操作員が所望のデータを検索するに際して、該操作員について機密保護のチェックを行う方法であって、前記項目及び／又は操作内容について、操作可能な範囲を定めた複数種類の権限を設定するとともに、各操作員について、前記各データ群毎に前記権限の種類を割り付け、データ検索時に、該操作員が所望した該データについての該操作員の権限をチェックし、該操作員が該データについて権限を有するならば該データの検索を可能と判定し、権限を有しないならば検索を不可能と判定することを特徴とするものである。

【０００７】また、請求項２に係る発明は、関連ある複数の項目についての１群のデータとして記憶した複数群のデータから操作員が所望のデータを検索するに際して、該操作員について機密保護のチェックを行う装置であって、前記項目及び／又は操作内容について、操作可

能な範囲を定めた複数種類の権限を設定するとともに、各操作員について、前記各データ群毎に前記権限の種類を割り付ける権限設定手段と、入力手段より入力された操作員の識別情報及び操作内容を受けて、前記権限設定手段から該操作員の権限を検索し、所望したデータの操作について該操作員が権限を有するならば該データの検索を可能と判定し、権限を有しないならば検索を不可能と判定する判定手段とから構成したことを特徴とするものである。

【０００８】

【作用】本発明の請求項１及び２の発明によれば、まず、権限設定手段により、データの項目及び／又は操作内容について、操作可能な範囲を定めた複数種類の権限を設定するとともに、各操作員について、各データ毎に前記権限の種類を割りつける。ついで、操作員は自身の識別情報及び操作内容を判定手段に入力する。判定手段はこれを受けて該操作員の権限を検索し、所望したデータの操作について該操作員が権限を有するならば、該データの検索を可能と判定し、権限を有しないならば検索不可能と判定する。

【０００９】以上のように本発明によれば、１人の操作員に対してデータ郡毎に異なる権限の設定が可能であり。その結果、データ郡毎に機密保護のチェックを行うことができ、全データについての機密保護チェックを行う必要がないため、機密保護のチェック処理を簡易且つ迅速に行うことができる。

【００１０】

【実施例】以下、本発明の実施例を添付図面に基づいて詳述する。図１は本発明の一実施例装置の概略を示す説明図である。この装置は文書データ等をファイルするファイリング装置であり、操作員（以下、「ユーザ」という）に関する機密保護のチェック機構を備えている。図１に示すように、この装置はＣＰＵ（１）と、記憶装置（５）と、入力装置（９）と、表示装置（１０）とを備えてなるものであり、ＣＰＵ（１）は権限登録部（２），権限検索／判定部（３）及び処理実行部（４）を備え、記憶装置（５）はデータ記憶部（６），権限情報記憶部（７）及び処理プログラム部（８）を備えている。以下、各部の詳細について説明する。尚、前記入力装置（９）はキーボード，マウス等よりなり、前記表示装置（１０）はディスプレイ等よりなるもので、いずれも公知の要素であるのでここではその詳しい説明を省略する。また、この例では、ファイルするデータを文書データとしているが、これに限るものではなく、数値データであっても問題ない。

【００１１】前記処理プログラム部（８）は所定の処理を実行するためのプログラムを格納するものであり、処理実行部（４）は指定された処理に対応したプログラムを前記処理プログラム部（８）より読み出して、当該プログラムを実行するものである。

【００１２】前記権限登録部（２）は前記入力装置（９）からの入力を受けてユーザの操作可能な範囲を定めた複数種類の権限を設定するとともに、各ユーザについて、前記権限の種類を割り付けるものである。当該権限登録部（２）の具体的な機能について、図２及び図３を用いて更に詳しく説明する。図２は権限の種類の設定について説明するための図表であり、図３は権限の割り付けについて説明するための図表である。尚、本例における文書データについてはテーマ毎（例えば顧客毎）に複数種の文書（見積書及び契約書）データが存在する。そしてこの「各文書データ」が前記請求項における「項目」に相当し、「テーマ毎の複数の文書データ」が前記請求項における「一群のデータ」に相当する。

【００１３】まず、権限設定について説明する。本例では図２に示すように、前記権限について「管理者権限」と「担当者権限」とを設け、それぞれその内容を設定している。即ち、「管理者権限」は見積書類の承認，契約書類の承認についての操作は可能であるが、見積書類の作成／変更，契約書類の作成／変更についての操作は不可能であるというものであり、「担当者権限」は見積書類の作成／変更，契約書類の作成／変更についての操作は可能であるが、見積書類の承認，契約書類の承認についての操作は不可能であるというものである。尚、ここにいう「作成」，「変更」，「承認」が請求項における「操作内容」に相当する。このように、権限設定は「文書データ」に係る「操作内容」の可否を設定することにより行われる。

【００１４】また、図３に示すように、各ユーザについて各テーマ毎に前記「管理者権限」を有するか、「担当者権限」を有するかを割り付けている。即ち、例えばユーザである「社員Ａ」はテーマ１については「担当者権限」を有し、テーマ２については「管理者権限」を有し、テーマ３については「管理者権限」及び「担当者権限」を有する。このように、権限の割り付けは各テーマについてユーザ毎に権限を割り付けることにより行われる。

【００１５】前記データ記憶部（６）はテーマ毎に前記文書データを記憶するものであり、前記権限情報記憶部（７）は前記権限登録部（２）で設定した権限情報を記憶するものである。

【００１６】前記権限検索／判定部（３）はユーザの識別情報及びテーマに関する情報を得、当該情報を基に前記権限情報記憶部（７）を検索して当該ユーザの権限情報を得、この権限情報を基に、ユーザの指定した文書データを当該ユーザが検索可能かどうかを判定するものである。

【００１７】この判定処理を図４を用いて更に詳しく説明する。同図に示すように、まず、ユーザである「社員Ａ」は入力装置（９）から自分のユーザー名及びパスワードを入力し、ログインを行う（ステップＳ１）。これ

により、権限検索／判定部（３）はユーザー名とパスワードによってユーザが「社員Ａ」であることを識別する。この時にユーザーに対するパスワードが正しくなければエラーとなりログインは不可能となる。ついで「社員Ａ」は自分の担当しているテーマの中から操作するテーマ（この例では「テーマ１」）を選択，入力する（ステップＳ２）。この入力を受けて権限検索／判定部（３）は前記権限情報記憶部（７）を検索して、「社員Ａ」の権限種を得、その権限内容を得る（ステップＳ３）。尚この際、「社員Ａ」は自身が権限を有しているテーマのみを選択可能であり、権限のない他のテーマは選択できないようになっている。図３に示すように、「社員Ａ」は「テーマ１」，「テーマ２」，「テーマ３」について権限を有し、「テーマ４」については権限を有しないので、「社員Ａ」は「テーマ１」，「テーマ２」，「テーマ３」についての選択はできるが、「テーマ４」についての選択はできない。図４の例では「テーマ１」を選択しており、権限検索／判定部（３）は権限情報記憶部（７）より「社員Ａ」の権限が「担当者権限」であるとの情報を得る。

【００１８】ついで「社員Ａ」は所望の操作内容を選択，入力する。これを受けて、権限検索／判定部（３）は前記権限情報記憶部（７）より得た権限内容と入力された操作内容とを照合して、「社員Ａ」が当該処理を操作可能であれば「操作可」の信号を処理実行部（４）に出力し、操作不可能であれば「操作不可」と表示装置（１０）に表示する。処理実行部（４）は選択された処理に対応した処理プログラムを記憶装置（５）の処理プログラム部（８）から読み出し、これを実行する（ステップＳ４）。図４の例では「社員Ａ」は見積書の作成若しくは変更又は契約書の作成若しくは変更の操作が可能であり、見積書の承認又は契約書の承認の操作は不可能である。

【００１９】図５はログイン後にテーマの切替を行う場合の例を示した説明図である。本例では、ログイン後いつでもテーマの切替を実施することができる。ログイン後のテーマ切替の際にもユーザが関係しない他のテーマについての操作は行えないようになっている。前述したように「社員Ａ」が選択可能なテーマは「テーマ１」，「テーマ２」，「テーマ３」であるため、「社員Ａ」はこれ以外の他のテーマについての操作は行えない。そしてテーマを切替ると、権限検索／判定部（３）はユーザの選択したテーマによって、そのユーザが当該テーマに対して割り当てられている権限を自動的に獲得し、権限の切替を行う。図５の例では「テーマ２」に切替ると権限が「管理者権限」に、「テーマ３」に切替ると権限が「管理者権限＋担当者権限」に自動的に切替られる。そして、ユーザはこの権限に応じた操作を行うことができる。

【００２０】以上の一連の処理を図６に示している。

【００２１】

【発明の効果】以上詳述したように本発明によれば、一人の操作員に対してデータ郡毎に異なる権限の設定が可能である。その結果、データ郡毎に機密保護のチェックを行うことができ、全データについての機密保護チェックを行う必要がないため、機密保護のチェック処理を簡易且つ迅速に行うことができる。また、一人の操作員に対して複数の権限を設定でき、より詳細な機密保護チェックが行えるとともに、異なる権限への移行を容易に行うことができ迅速な操作を行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施例装置の概略構成を示すブロック図である。

【図２】権限の種類について説明するための説明図である。

【図３】権限の割り付けについて説明するための説明図である。

【図４】判定処理を説明するための説明図である。

【図５】ログイン後におけるテーマの切替えについて説明するための説明図である。

【図６】判定処理及びテーマの切替え処理を示すフローチャートである。

【図７】ＩＤコード等と権限との関係を示す図表である。

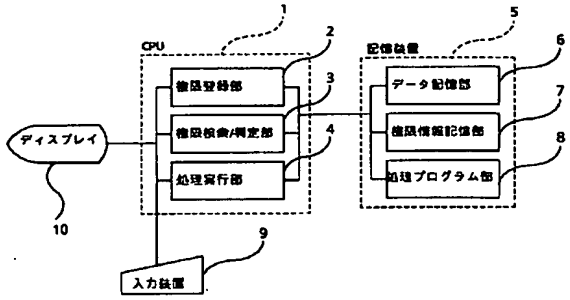
【図８】権限の種類について説明するための説明図である。

【図９】従来の機密保護チェック処理を示す説明図である。

【符号の説明】

１　ＣＰＵ
２　権限登録部
３　権限検索／判定部
４　処理実行部
５　記憶装置
６　データ記憶部
７　権限情報記憶部
８　処理プログラム部
９　入力装置
１０　表示装置

【図１】



【図２】

権限毎の操作可能範囲

	管理者権限	担当者権限
見積書類の作成/変更	不可	可
見積書類の承認	可	不可
契約書類の作成/変更	不可	可
契約書類の承認	可	不可

【図３】

操作員のテーマ毎の権限

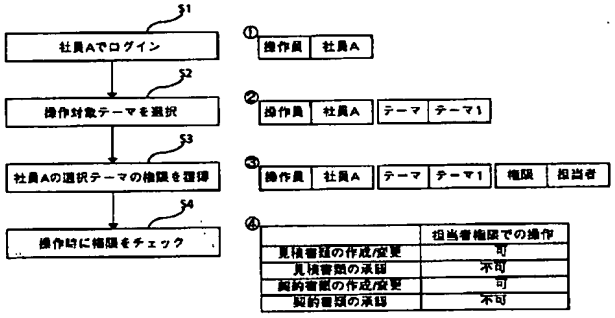
	テーマ1	テーマ2	テーマ3	テーマ4
社員A	担当者	管理者	管理者/担当者	
社員B	管理者	担当者	担当者	
社員C	担当者	担当者	担当者	

【図７】

操作員のパスワード毎の権限

操作員ID	パスワード	操作権限
社員A	123	担当者
社員A	124	管理者
社員B	456	管理者
社員C	789	担当者

【図４】

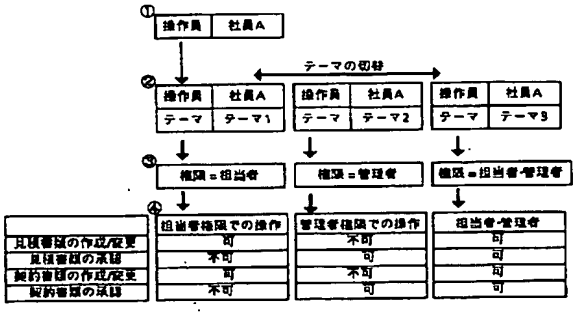


【図８】

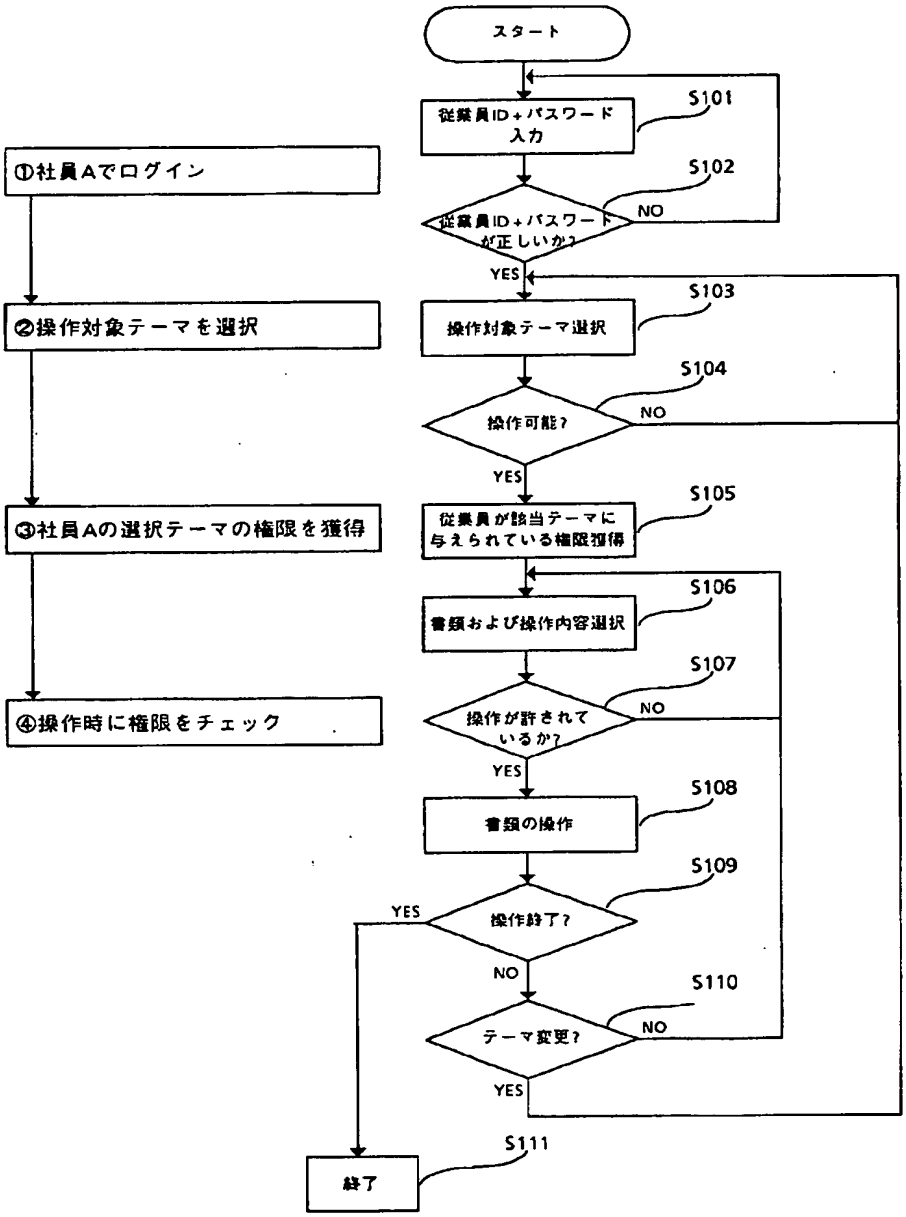
権限毎の操作可能範囲

	管理者権限	担当者権限
見積書類の作成/変更	不可	可
見積書類の承認	可	不可
契約書類の作成/変更	不可	可
契約書類の承認	可	不可

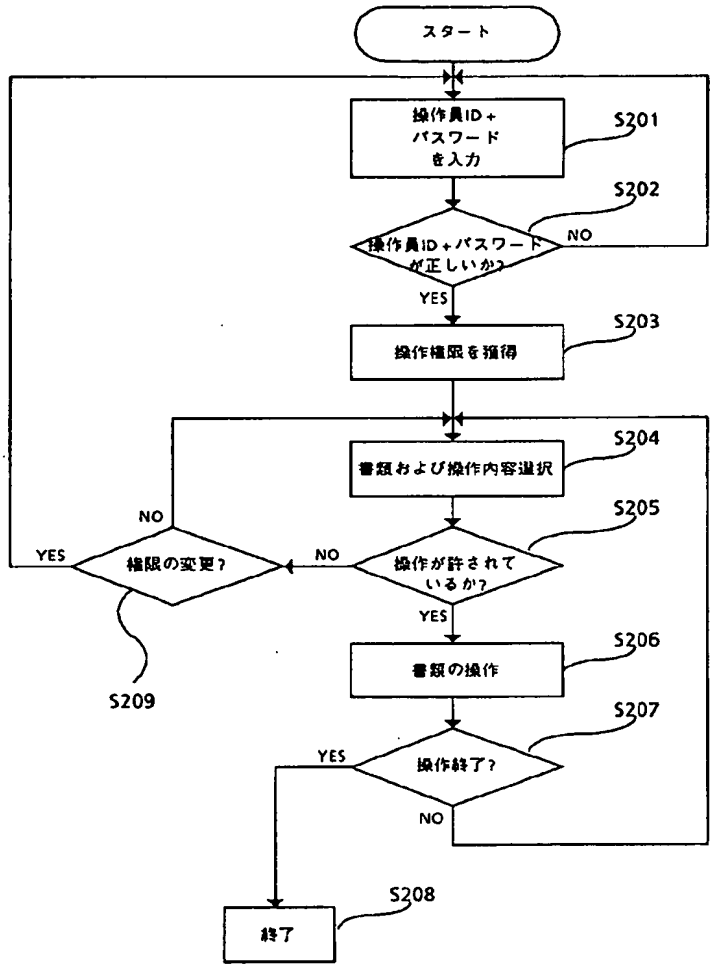
【図５】



【図6】


スタート
従業員ID＋パスワード入力
S101
従業員ID＋パスワードが正しいか?
S102
NO
YES
操作対象テーマ選択
S103
操作可能?
S104
NO
YES
従業員が該当テーマに与えられている権限獲得
S105
書類および操作内容選択
S106
操作が許されているか?
S107
NO
YES
書類の操作
S108
操作終了?
S109
YES
NO
テーマ変更?
S110
NO
YES
終了
S111
①社員Aでログイン
②操作対象テーマを選択
③社員Aの選択テーマの権限を獲得
④操作時に権限をチェック

【図9】


スタート
操作員ID＋
パスワード
を入力
S201
S202
操作員ID＋パスワード
が正しいか?
NO
YES
S203
操作権限を獲得
S204
書類および操作内容選択
S205
操作が許されて
いるか?
NO
YES
権限の変更?
NO
YES
S209
S206
書類の操作
S207
操作終了?
YES
NO
S208
終了